REMARKS

Claims 1-35 are currently pending in the subject application and are presently under consideration. Claims 1, 12, 20, 28 and 33-35 have been amended as shown on pp. 2-8 of the Reply.

Applicants' representative thanks the Examiner for the courtesies extended during the teleconference of April 2, 2007.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claim 12 Under 35 U.S.C. §112, second paragraph

Claim 12 stands rejected under 35 U.S.C. §112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, claim 12 has been rejected for having insufficient antecedent basis for the limitation "a sequence". Claim 12 has been amended to correct any deficiencies related to this rejection, as such the rejection is moot and should be withdrawn.

II. Rejection of Claims 1-4, 19, 28, 30, 31 and 33-35 Under 35 U.S.C. §102(e)

Claims 1-4, 19, 28, 30, 31 and 33-35 stand rejected under 35 U.S.C. §102(e) as being anticipated by Gligor *et al.* (US Patent 6,973,187). It is respectfully requested that this rejection should be withdrawn for at least the following reasons. Gligor *et al.* does not teach or suggest each and every element as set forth in the subject claims.

> A single prior art reference anticipates a patent claim only if it expressly or inherently describes each and every limitation set forth in the patent claim. *Trintec Industries, Inc. v. Top-U.S.A. Corp.*, 295 F.3d 1292, 63 USPQ2d 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the ... claim. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

The claimed subject matter relates to a first code that is designed within the noise model, and performs various algebraic transformations on such first code to create a second code. Upon

transforming the first code into the second code, the second code will appear to be random to a computationally bounded adversary. Therefore an adversarial attack on the second code will essentially be a noise attack on the first code, as the attack will be randomly distributed across the first code. Randomly distributing the attack across the first code allows the code to act as it was designed – with respect to random noise. Thus the first code can be associated with error correction/detection properties when random noise is applied to the first code.

Independent claims 1, 28 and 33-35 recite a system that facilitates efficient code construction, comprising: *a component that receives a first code,* ***the first code comprises algorithms utilized to correct noise errors with high probability****; and a transformation component that transforms the first code to a new code that has essentially same length parameters as the first code but is hidden to a computationally bounded adversary, the transformation component utilizes a random number generator to perform algebraic transformations on data utilizing the first code to generate the new code,* ***wherein the new code acts as a protective wrapping of the first code, such that an attack on the new code by the computationally bounded adversary would appear as a noise attack on the first code***. Gligor *et al.* does not expressly or inherently disclose the aforementioned novel aspects of applicants' claimed subject matter as recited in the subject claims.

Gligor *et al.* discloses a method for providing both data confidentiality and integrity for a message. The method includes receiving an input plaintext string and padding it as necessary such that its length is a multiple of 1 bits; partitioning the input plaintext string a length that is a multiple of 1 bits into a plurality of equal-size blocks of 1 bits in length; creating an MDC block of 1 bits in length that includes the result of applying a non-cryptographic Manipulation Detection Code (MDC) function to the plurality of the equal-size blocks; making one and only one processing pass with a single cryptographic primitive over each of the equal-size blocks and the MDC block to create a plurality of hidden ciphertext blocks each of 1 bits in length; and performing a randomization function over the plurality of hidden ciphertext blocks to create a plurality of output ciphertext blocks each of 1 bits in length. (*See* col. 6, lines 37-53).

In contrast, applicants' claimed subject matter discloses a system that includes a code generator/encoder that creates a code 1 designed in the noise model. Code 1 is delivered to a code hiding module that includes a random number generator. The code hiding module

effectively hides code 1 *via* randomizing data that employs code 1, thereby not enabling an adversary to determine a location of critical bits to attack. More particularly, the code hiding module utilizes the random number generator to perform algebraic transformations on data utilizing code 1. A code 2 results from these algebraic transformations, wherein the code 2 is a transformed version of the code 1.

Code 2 is then received by a decoder that can decode code 2 and determine the code 1. Thus, code 2 can be viewed as a protective wrapping of code 1 as illustrated with respect to Fig. 1. The decoder has access to algorithms utilized by the code hiding module, and can thus decode code 2 and determine code 1. Furthermore, if an adversary had directed an attack on code 2, upon decoding such adversarial attack would appear as a noise attack on code 1. Thereafter, as code 1 includes algorithms utilized to correct noise errors with high probability, such errors are corrected with a high success rate when compared to conventional codes designed in the adversarial model. (*See* pg. 7, line15-pg. 8, line 22).

Gligor *et al.* does not expressly or inherently disclose a system that generates a new code by randomizing data that employs the first code, wherein the first code includes algorithms utilized to correct noise errors with high probability. Gligor *et al.* simply provides a block encryption method that provides data confidentiality with a single cryptographic primitive and a single processing pass over the input plaintext string by using a non-cryptographic MDC function. Accordingly, Gligor *et al.* is silent with regard to a system that facilitates efficient code construction …, ***wherein the new code acts as a protective wrapping of the first code, such that an attack on the new code by the computationally bounded adversary would appear as a noise attack on the first code***.

In view of at least the above, it is readily apparent that Gligor *et al.* fails to expressly or inherently disclose applicants' claimed subject matter as recited in independent claims 1, 28 and 33-35 (and claims 2-4, 19, 30 and 31 which respectively depend there from). Accordingly, it is respectfully requested that these claims be deemed allowable.

III. Rejection of Claim 32 Under 35 U.S.C. §103(a)

Claim 32 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Gligor *et al.* It is respectfully submitted that this rejection should be withdrawn for the following reasons.

Gligor *et al.* does not teach or suggest each and every element set forth in the subject claims. In particular, Gligor *et al.* does not make up for aforementioned deficiencies with respect to independent claim 28 (which claim 32 depends respectively there from). Thus, the claimed subject matter as recited in claim 32 is not obvious over Gligor *et al.* Therefore, it is respectfully submitted that this rejection be withdrawn.

IV. Rejection of Claims 5-8, 11-18, 20-23 and 29 Under 35 U.S.C. §103(a)

Claims 5-8, 11-18, 20-23 and 29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Gligor *et al.* in view of Bohnke *et al.* (US Patent 6,557,139). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Gligor *et al.*, and Bohnke *et al.,* individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

> To reject claims in an application under §103, an examiner must establish a *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See* MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicants' disclosure. *See In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

As stated *supra*, the claimed subject matter relates to a first code that is designed within the noise model, and performs various algebraic transformations on such first code to create a second code. Upon transforming the first code into the second code, the second code will appear to be random to a computationally bounded adversary. Therefore an adversarial attack on the second code will essentially be a noise attack on the first code, as the attack will be randomly distributed across the first code. Randomly distributing the attack across the first code allows the code to act as it was designed – with respect to random noise. Thus the first code can be associated with error correction/detection properties when random noise is applied to the first

code.

Independent claim 20 recites a system that hides a codeword from a computationally bounded adversary, comprising: *a code generator that generates a first code based at least in part upon a sequence of messages that are desirably relayed to a receiver,* ***the first code comprising algorithms utilized to correct noise errors with high probability****; a code hiding module that creates a second code, the second code being a pseudo random version of the first code, the second code appears to be random to a computationally bounded adversary; and a decoder that determines the first code from the second code,* ***wherein the second code acts as a protective wrapping of the first code, such that an attack on the second code by the computationally bounded adversary would appear as a noise attack on the first code****.*

Gligor *et al.* discloses a method for providing both data confidentiality and integrity for a message. The method includes receiving an input plaintext string and padding it as necessary such that its length is a multiple of 1 bits; partitioning the input plaintext string a length that is a multiple of 1 bits into a plurality of equal-size blocks of 1 bits in length; creating an MDC block of 1 bits in length that includes the result of applying a non-cryptographic Manipulation Detection Code (MDC) function to the plurality of the equal-size blocks; making one and only one processing pass with a single cryptographic primitive over each of the equal-size blocks and the MDC block to create a plurality of hidden ciphertext blocks each of 1 bits in length; and performing a randomization function over the plurality of hidden ciphertext blocks to create a plurality of output ciphertext blocks each of 1 bits in length. (*See* col. 6, lines 37-53).

In contrast, applicants' claimed subject matter discloses a system that includes a code generator/encoder that creates a code 1 designed in the noise model. Code 1 is delivered to a code hiding module that includes a random number generator. The code hiding module effectively hides code 1 *via* randomizing data that employs code 1, thereby not enabling an adversary to determine a location of critical bits to attack. More particularly, the code hiding module utilizes the random number generator to perform algebraic transformations on data utilizing code 1. A code 2 results from these algebraic transformations, wherein the code 2 is a transformed version of the code 1.

Code 2 is then received by a decoder that can decode code 2 and determine the code 1. Thus, code 2 can be viewed as a protective wrapping of code 1 as illustrated with respect to Fig.

1. The decoder has access to algorithms utilized by the code hiding module, and can thus decode code 2 and determine code 1. Furthermore, if an adversary had directed an attack on code 2, upon decoding such adversarial attack would appear as a noise attack on code 1. Thereafter, as code 1 includes algorithms utilized to correct noise errors with high probability, such errors are corrected with a high success rate when compared to conventional codes designed in the adversarial model. (*See* pg. 7, line15-pg. 8, line 22).

Gligor *et al.* does not expressly or inherently disclose a system that generates a new code by randomizing data that employs the first code, wherein the first code includes algorithms utilized to correct noise errors with high probability. Gligor *et al.* simply provides a block encryption method that provides data confidentiality with a single cryptographic primitive and a single processing pass over the input plaintext string by using a non-cryptographic MDC function. Accordingly, Gligor *et al.* is silent with regard to a system that hides a codeword from a computationally bounded adversary *…, **wherein the second code acts as a protective wrapping of the first code, such that an attack on the second code by the computationally bounded adversary would appear as a noise attack on the first code***.

Bohnke *et al.* does not cure the deficiencies of Gligor *et al.* with respect to independent claim 20. Bohnke *et al.* was cited by the examiner for disclosing a decoder. (See Office Action dated 2-13-07, pg. 14). Accordingly, Bohnke *et al.* is silent with respect to a system that hides a codeword from a computationally bounded adversary *…, **wherein the second code acts as a protective wrapping of the first code, such that an attack on the second code by the computationally bounded adversary would appear as a noise attack on the first code***.

In view of the aforementioned deficiencies of Gligor *et al.* and Bohnke *et al.*, it is respectfully submitted that this rejection be withdrawn with respect to independent claims 1, 20, and 28 (and claims 5-8, 11-18, 21-23 and 29 that depend there from).

V. Rejection of Claims 9, 10, 24 and 25 Under 35 U.S.C. §103(a)

Claims 9, 10, 24 and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Gligor *et al.* in view of Bohnke *et al.*, and further in view of Guruswami (Foundations of Computer Science, 2001, Proceedings, 42nd IEEE Symposium, Pages: 658-667, ISBN: 0-7695-1116-3). It is respectfully submitted that this rejection should be withdrawn for the following

reasons. Gligor *et al.*, Bohnke *et al.,* and Guruswami, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Guruswami does not make up for aforementioned deficiencies of Gligor *et al.* and Bohnke *et al.* with respect to independent claim 1 (which claims 9, 10, 24 and 25 depend respectively there from). Thus, the claimed subject matter as recited in claims 9, 10, 24 and 25 is not obvious over the combination of Gligor *et al.*, Bohnke *et al.* and Guruswami. Therefore, it is respectfully submitted that this rejection be withdrawn.

VI. Rejection of Claims 26 and 27 Under 35 U.S.C. §103(a)

Claims 26 and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Gligor *et al.* in view of Bohnke *et al.*, and further in view of Lee *et al.* (U.S. Patent 6,792,542). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Gligor *et al.*, Bohnke *et al.,* and Lee *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Lee *et al.* does not make up for aforementioned deficiencies of Gligor *et al.* and Bohnke *et al.* with respect to independent claim 20 (which claims 26 and 27 depend respectively there from). Thus, the claimed subject matter as recited in claims 26 and 27 is not obvious over the combination of Gligor *et al.*, Bohnke *et al.* and Lee *et al.* Therefore, it is respectfully submitted that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP588US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,
AMIN, TUROCY & CALVIN, LLP

/Marisa J. Zink/
Marisa J. Zink
Reg. No. 48,064

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone: (216) 696-8730
Facsimile: (216) 696-8731